THREAT BULLETINS

Microsoft Releases New Report on Silk Typhoon's Evolving TTPs

TLP:WHITE

Mar 06, 2025

On March 5, 2025, Microsoft released a report identifying the Silk Typhoon's evolving tactics. Silk Typhoon, also known as Hafnium, is a sophisticated Chinese state-sponsored threat actor known for its extensive espionage activities. The group is known for the exploitation of zero-day vulnerabilities in edge devices, targeting a wide array of sectors globally, such as Information Technology (IT), health, education, and government. Recently, the group shifted to target IT solutions like remote management tools and cloud applications to gain initial access, causing supply chain disruptions.

Silk Typhoon is seen as a significant threat to critical infrastructure, particularly through their focus on supply chain attacks. This method allows them to compromise multiple targets by infiltrating a single point of entry within the supply chain. Their persistent use of zero-day vulnerabilities indicates high sophistication and access to advanced resources. The transition from on-premises to cloud environments suggests an adaptation to modern IT architectures, increasing the potential impact of their operations.

The group compromises supply chains by stealing API keys from cloud app providers, which allows them access to downstream customer environments. The group has also been using password spray attacks and leveraging leaked password repositories published

on GitHub to gain access to corporate accounts. Most recently, in January 2025, the threat actor leveraged the Ivanti Pulse Connect VPN flaw tracked as CVE-2025-0282. The various compromise techniques demonstrate the group's diverse skills and tools, emphasizing its threat.

This report is shared for your situational awareness, as health is an affected sector. Health-ISAC advises familiarizing yourself with the threat actor's Tactics, Techniques, and Procedures (TTPs) and applying the recommendations from the following section.

Recommendations:

Health-ISAC provides this information to prevent your security apparatus's successful exploitation and disruption. For more information, see Health Industry Cybersecurity Practices (HICP): Managing Threats and Protecting Patients.

- Ensure all public-facing devices are regularly patched.
- Establish strong controls for identities and review privileges for all users and applications.
- Build strong credential practices, apply the principle of least privilege, and limit credential exposure when possible.
- Limit access controls and use multi-factor authentication (MFA).
- Segment networks and continuously monitor for signs of suspicious activity.
- Ensure sensitive data is stored securely.
- Ensure that an Incident Response and Business Continuity Plan is in place to minimize operation disruption in case of a cyberattack.

Reference(s)	, Tech Radar, The Hacker News, Mitre, , thecyberexpress, HHS, Microsoft Blog

Sources

https://www.microsoft.com/en-us/security/blog/2025/03/05/silk-typhoon-targeting-it-supply-chain/
https://thecyberexpress.com/silk-typhoon-campaign/
https://www.techradar.com/pro/security/microsoft-says-chinese-silk-typhoon-hackers-are-targeting-cloud-and-it-apps-to-steal-business-data
https://theedgemalaysia.com/node/746926
https://thehackernews.com/2025/03/china-linked-silk-typhoon-expands-cyber.html
https://www.redlegg.com/blog/threat-profile-brsilk-typhoon
https://attack.mitre.org/groups/G0125/

Incident Date
Mar 06, 2025 (UTC)

Alert ID 8f9e4206

This Alert has 1 attachment(s). To view or download the attachment(s), click "View Alert" to login to the web portal.

View Alert

Share Feedback

was this helpful? |

Tags Silk Typhoon, HAFNIUM, Microsoft

TLP:WHITE Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

For Questions or Comments
Please email us at toc@h-isac.org

Download Health-ISAC's Information Sharing App.

For more updates and alerts, visit: **https://health-isac.cyware.com/webapp/**